LDPC Codes for Post-Quantum Cryptography

PRESENTED BY:

David Mitchell, New Mexico State University, dgmm@nmsu.edu
ABOUT ME

Background:

• B.Sc. Mathematics, Ph.D. EE (University of Edinburgh, UK). Post-doc/Visiting Assistant Professor at University of Notre Dame.

• Error correcting codes, information theory, iterative information processing, data compression

• Post-doc: Yanfang Liu (URLLC in 5G, FPGA implementation), Phd students: Andrew Cummins (Wireless technologies in smart grid), Ahmad Golmohammadi (Distributed source coding)

Keywords:

Graph based codes, LDPC codes, iterative decoding, wireless communications, 5G, spatially coupled codes
MOTIVATION

Essentially all cryptographic protocols today make use of number theory (RSA, ElGamal, DSA, Diffie-Hellman, …)
Essentially all cryptographic protocols today make use of number theory (RSA, ElGamal, DSA, Diffie-Hellman, …)

Any such protocol is vulnerable with the advent of quantum computers (and related quantum algorithms [1,2])


Essentially all cryptographic protocols today make use of number theory (RSA, ElGamal, DSA, Diffie-Hellman,...)

Any such protocol is vulnerable with the advent of quantum computers (and related quantum algorithms [1,2])

According to NIST [3], the most promising candidates for post-quantum cryptography are:

- Code-based cryptosystems (McEliece/Niederreiter)
- Lattice-based cryptosystems

BACKGROUND: LINEAR CODES

A digital communications system:

\[
\begin{array}{c}
\text{Encoder} \quad \text{Noisy} \\
u \quad v \\
\text{information} \quad \text{transmitted} \\
\text{sequence} \quad \text{code sequence} \\
\end{array} \rightarrow \begin{array}{c}
\text{Noisy} \\
\text{Channel} \\
r \\
\text{received} \quad \text{estimated} \\
\text{sequence} \quad \text{code sequence} \\
\end{array} \rightarrow \begin{array}{c}
\text{Decoder} \\
\hat{u} \\
\end{array}
\]
A digital communications system:

- **Encoder**
  - Input: Information sequence \( u \)
  - Output: Transmitted code sequence \( v \)

- **Noisy Channel**
  - Input: Transmitted code sequence \( v \)
  - Output: Received code sequence \( r \)

- **Decoder**
  - Input: Received code sequence \( r \)
  - Output: Estimated code sequence \( \hat{u} \)

- **Add Redundancy**
  - \( k \) bits added to ensure redundancy

- **Error Correction**
  - \( n \) bits estimated to correct errors

Example:
- Information sequence: \( k \)
- Transmitted code sequence: \( n \)
- Received code sequence: \( 010 \)
- Estimated code sequence: \( 0 \)
BACKGROUND: LINEAR CODES

- A digital communications system:

  ![Diagram of communication system](Image)

  - **Encoder** takes an information sequence and adds redundancy to create a transmitted code sequence.
  - **Noisy Channel** introduces noise, resulting in a received code sequence.
  - **Decoder** attempts to estimate the original code sequence by correcting errors.

  - Example: Encoding as \( \mathbf{v}_{1\times n} = \mathbf{u}_{1\times k} \mathbf{G}_{k\times n} \) (Ex: \( k = 1, n = 3, \mathbf{G} = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} \))
**BACKGROUND: LINEAR CODES**

- A digital communications system:

  ![Diagram](image)

  - **Encoder**\[\mathbf{u} \rightarrow \mathbf{v}\]
  - **Noisy Channel**\[\mathbf{v} \rightarrow \mathbf{r}\]
  - **Decoder**\[\mathbf{r} \rightarrow \hat{\mathbf{u}}\]

  - Information sequence: \[\mathbf{u}\]
  - Transmitted code sequence: \[\mathbf{v}\]
  - Received sequence: \[\mathbf{r}\]
  - Estimated code sequence: \[\hat{\mathbf{u}}\]

  - **Add redundancy**
  - \[\frac{k}{n} \rightarrow \frac{0}{000}\]

  - **Error correction**
  - \[\frac{0}{10} \rightarrow \frac{0}{0}\]

- Encoding is achieved as \[\mathbf{v}_{1 \times n} = \mathbf{u}_{1 \times k} \mathbf{G}_{k \times n}\]
  (Ex: \(k = 1, n = 3, \mathbf{G} = [1 1 1]\))

- What is the cost of redundancy?

- **Efficiency** – the code rate is \(R = \frac{k}{n}\)

Research Spotlight Forum
McELIECE CRYPTOSYSTEM

- McEliece proposed a code-based cryptosystem based on algebraic Goppa codes [4]

McELIECE CRYPTOSYSTEM

- McEliece proposed a code-based cryptosystem based on algebraic Goppa codes [4]
  - Decoding a random linear code cannot be solved in polynomial time [5]

McEliece proposed a code-based cryptosystem based on algebraic Goppa codes [4]

- Decoding a random linear code cannot be solved in polynomial time [5]
- Many families of structured (Goppa, Reed-Solomon, …) and semi-structured (low-density parity-check) linear codes have polynomial-time decoding algorithms

McEliece proposed a code-based cryptosystem based on algebraic Goppa codes [4]

- Decoding a \textbf{random} linear code cannot be solved in polynomial time [5]
- Many families of structured (Goppa, Reed-Solomon, ...) and semi-structured (low-density parity-check) linear codes have polynomial-time decoding algorithms

Private key: \[ \begin{align*}
\text{generator matrix} \quad & G \\
\text{non-singular “scrambling” matrix} \quad & S \\
\text{permutation matrix} \quad & P
\end{align*} \]

---


McELIECE CRYPTOSYSTEM

- McEliece proposed a code-based cryptosystem based on algebraic Goppa codes [4]
  - Decoding a random linear code cannot be solved in polynomial time [5]
  - Many families of structured (Goppa, Reed-Solomon, …) and semi-structured (low-density parity-check) linear codes have polynomial-time decoding algorithms

Private key:  \( k \times n \) generator matrix \( G \)
  - random dense \( k \times k \) non-singular “scrambling” matrix \( S \)
  - random dense \( n \times n \) permutation matrix \( P \)

Public key:  random-like \( k \times n \) generator matrix \( G' = SGP \)

Initial proposal: Form Goppa code of length $n = 2^m$ from an irreducible polynomial of degree $t$ over $\text{GF}(2^m)$

- Probability $\sim 1/t$ of choosing an irreducible polynomial
- Number of irreducible polynomials $\sim n^t/t$
- Decoder can correct $t$ errors in polynomial time
ENCRYPTION

- Initial proposal: Form Goppa code of length \( n = 2^m \) from an irreducible polynomial of degree \( t \) over GF(\( 2^m \))

- Probability \( \sim 1/t \) of choosing an irreducible polynomial

- Number of irreducible polynomials \( \sim n^t/t \)

- Decoder can correct \( t \) errors in polynomial time

Encryption:

\[ x = uG' + e \]

- \( k \)-bit block
- Random error pattern (\( \leq t \) errors)
- Public key
Decryption:

1) Compute $x' = x \cdot P^{-1} =$

$$= (u \cdot S \cdot G \cdot P + e) \cdot P^{-1} =$$

$$= u \cdot S \cdot G + e \cdot P^{-1}$$

Codeword in secret code  Permutated error pattern ($\leq t$ errors)
DECYPHER

Decryption:

1) Compute $x' = x \cdot P^{-1} =$

$= (u \cdot S \cdot G \cdot P + e) \cdot P^{-1} =$

$= u \cdot S \cdot G + e \cdot P^{-1}$

Codeword in secret code \hspace{2cm} Permuted error pattern ($\leq t$ errors)

2) Decode to obtain

$u' = uS$
DECRYPTION

Decryption:

1) Compute \( x' = x \cdot P^{-1} = \)
\[ = (u \cdot S \cdot G \cdot P + e) \cdot P^{-1} = \]
\[ = u \cdot S \cdot G + e \cdot P^{-1} \]

[Cross-reference: Codeword in secret code][Permuted error pattern (\( \leq t \) errors)]

2) Decode to obtain
\( u' = uS \)

3) Compute
\( u = u'S^{-1} \)
The most promising attack on the original McEliece cryptosystem employs information set decoding (ISD).
The most promising attack on the original McEliece cryptosystem employs information set decoding (ISD).

Post-quantum algorithms, such as Grover's database search, can be used to speed up attacks.

Grover's algorithm reduces the number of iterations of attack, but not the cost per iteration.

[Figure created by Marco Baldi]
# ADVANTAGES AND DISADVANTAGES

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>The McEliece cryptosystem is still <strong>unbroken</strong> (both pre- and post- quantum attacks)</td>
<td>Requires <strong>large public keys</strong> (56 KiB or more for 80-bit security)</td>
</tr>
<tr>
<td>System is 2-3 orders of magnitude <strong>faster</strong> than competitors (RSA, Diffie-Hellman, DSA)</td>
<td><strong>Low information rate</strong> (for DSA) – ciphertext longer than cleartext</td>
</tr>
<tr>
<td>Conversions of the system exist that achieve <strong>CCA2 security</strong></td>
<td></td>
</tr>
</tbody>
</table>
LDPC Codes

Low-density parity-check (LDPC) codes are defined on a large (random-like) sparse graph

5G data, DVB-S2, ITU-T G.hn standard (data networking over power lines, phone lines, and coaxial cables), 10GBase-T Ethernet, Wi-Fi standards 802.11,...
Low-density parity-check (LDPC) codes are defined on a large (random-like) sparse graph.

- 5G data, DVB-S2, ITU-T G.hn standard (data networking over power lines, phone lines, and coaxial cables), 10GBase-T
- Ethernet, Wi-Fi standards 802.11,...

Capacity approaching under belief propagation (BP)

Decoding. Complexity of encoding and decoding is linear in codeword length.
LDPC Codes

- Low-density parity-check (LDPC) codes are defined on a large (random-like) sparse graph.

- 5G data, DVB-S2, ITU-T G.hn standard (data networking over power lines, phone lines, and coaxial cables), 10GBase-T Ethernet, Wi-Fi standards 802.11,...

- Capacity approaching under belief propagation (BP) decoding

- Complexity of encoding and decoding is linear in codeword length

Warning! Public key cannot also be sparse or else the secret key can be obtained!
CODES ON GRAPHS

\[ u \xrightarrow{Encoder} v \xrightarrow{Noisy \ Channel} r \xrightarrow{Decoder} \hat{u} \]
CODES ON GRAPHS

\[
\begin{align*}
\text{message} & \quad \text{codeword} \\
\mathbf{u} & \quad \mathbf{v} = [v_1, v_2, v_3, v_4] \\
0 & \quad \rightarrow \quad 0000 \\
1 & \quad \rightarrow \quad 1101 \\
R & = 1/4
\end{align*}
\]
CODES ON GRAPHS

\[ u \xrightarrow{\text{Encoder}} v \xrightarrow{\text{Noisy Channel}} r \xrightarrow{\text{Decoder}} \hat{u} \]

**Code**

<table>
<thead>
<tr>
<th>message</th>
<th>codeword</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0 0 0 0</td>
</tr>
<tr>
<td>1</td>
<td>1 1 0 1</td>
</tr>
</tbody>
</table>

\[ R = 1/4 \]

**Code Graph**

- \( v_1 + v_2 + v_3 = 0 \)
- \( v_1 + v_3 + v_4 = 0 \)
- \( v_2 + v_3 + v_4 = 0 \)
CODES ON GRAPHS

Message codeword
\[ u \rightarrow v = [v_1 v_2 v_3 v_4] \]

0 \rightarrow 0 0 0 0
1 \rightarrow 1 1 0 1

\[ R = 1/4 \]

Decoder
Encoder
Noisy Channel

\[ v_1 + v_2 + v_3 = 0 \]
\[ v_1 + v_3 + v_4 = 0 \]
\[ v_2 + v_3 + v_4 = 0 \]
LDPC codes can be decoded with low complexity using **iterative message passing decoding** (exchanging messages in the graph)
EXAMPLE: ITERATIVE DECODING

received (corrupted) codeword

1 0 0 1

\[ V_1 + V_2 + V_3 \]

\[ V_1 + V_3 + V_4 \]

\[ V_2 + V_3 + V_4 \]
Iteration 1: bit-to-check

EXAMPLE: ITERATIVE DECODING
Iteration 1: bit-to-check

1 + 0 + v_3

1 + 0

1 + v_3 + v_4

0 + v_3 + v_4
Iteration 1: bit-to-check

1 + 0 + 0 = 1 ??
1 + 0 + v₄
0 + 0 + v₄
Iteration 1: bit-to-check

EXAMPLE: ITERATIVE DECODING

1 + 0 + 0 = 1 ??
1 + 0 + 1 = 0 ✓
0 + 0 + 1 = 1 ??

Research Spotlight Forum
Iteration 1: check-to-bit

1 + 0 + 0 = 1 ??

1 + 0 + 1 = 0 ✓

0 + 0 + 1 = 1 ??
Iteration 1: check-to-bit

EXAMPLE: ITERATIVE DECODING

1+0+0=1 ??
1+0+1=0 ✓
0+0+1=1 ??
EXAMPLE: ITERATIVE DECODING

**Iteration 1: check-to-bit**

1. \(1 + 0 + 0 = 1 \) ??
2. \(1 + 0 + 1 = 0 \)  
   
3. \(0 + 0 + 1 = 1 \) ??
Iteration 1: bit processing

EXAMPLE: ITERATIVE DECODING

1 + 0 + 0 = 1 ??
1 + 0 + 1 = 0 ✓
0 + 0 + 1 = 1 ??
EXAMPLE: ITERATIVE DECODING

Iteration 2: bit-to-check

\[ v_1 + v_2 + v_3 \]

\[ v_1 + v_3 + v_4 \]

\[ v_2 + v_3 + v_4 \]
Iteration 2: bit-to-check

1

1

1 + v_2 + v_3

1 + v_3 + v_4

v_2 + v_3 + v_4
EXAMPLE: ITERATIVE DECODING

Iteration 2: bit-to-check

\[
\begin{align*}
1 & + 1 + v_3 \\
1 & + v_3 + v_4 \\
1 & + v_3 + v_4
\end{align*}
\]
EXAMPLE: ITERATIVE DECODING

Iteration 2: bit-to-check

1 + 1 + 0 = 0 ✓
1 + 0 + v_4
1 + 0 + v_4
EXAMPLE: ITERATIVE DECODING

**Iteration 2: bit-to-check**

1+1+0=0 ✓ 1+0+1=0 ✓ 1+0+1=0 ✓
Iteration 2: check-to-bit

Example:

ITERATIVE DECODING
Iteration 2: check-to-bit

EXAMPLE: ITERATIVE DECODING
EXAMPLE: ITERATIVE DECODING

Iteration 2: check-to-bit

1
Stay, Stay

1
Stay, Stay

0
Stay, Stay, Stay

1
Stay, Stay

1+1+0=0 ✓

1+0+1=0 ✓

1+0+1=0 ✓
EXAMPLE: ITERATIVE DECODING

decoded codeword

\[
\begin{array}{cccc}
1 & 1 & 0 & 1 \\
\end{array}
\]

\[
\begin{array}{cccc}
1+1+0=0 & 1+0+1=0 & 1+0+1=0 \\
\end{array}
\]
LDPC codes can be decoded with low complexity using iterative message passing decoding (exchanging messages in the graph)
QUASI-CYCLIC (QC) LDPC CODES

QC-LDPC/QC-MDPC codes are “structured” LDPC codes that facilitate efficient implementation.

\[
\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
\]
**QUASI-CYCLIC (QC) LDPC CODES**

QC-LDPC/QC-MDPC codes are “structured” LDPC codes that facilitate efficient implementation.

In this example, the matrix is a $1 \times 3$ array of $7 \times 7$ circulant matrices. It can be completely described by row 1.

$$
\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
$$
QUASI-CYCLIC (QC) LDPC CODES

QC-LDPC/QC-MDPC codes are “structured” LDPC codes that facilitate efficient implementation.

In this example, the matrix is a 1 x 3 array of 7 x 7 circulant matrices. It can be completely described by row 1.

Key sizes are reduced!
QUASI-CYCLIC (QC) LDPC CODES

QC-LDPC/QC-MDPC codes are “structured” LDPC codes that facilitate efficient implementation.

In this example, the matrix is a 1 x 3 array of 7 x 7 circulant matrices. It can be completely described by row 1.

Key sizes are reduced!

A decoding error attack [6] can build up the distance spectrum of the QC-MDPC code to recover the secret key.

RESEARCH QUESTIONS

Can robust QC-MDPC or QC-LDPC codes be designed that are resilient to key-recovery attacks like [6]?

RESEARCH QUESTIONS

Can robust QC-MDPC or QC-LDPC codes be designed that are resilient to key-recovery attacks like [6]?

Instead of adding binary noise (error) vectors, can we add real-valued noise to the encryption?

- We can take advantage of soft-decision decoding of LDPC codes
- Can soft information be exploited by attackers?

Can robust QC-MDPC or QC-LDPC codes be designed that are resilient to key-recovery attacks like [6]?

Instead of adding binary noise (error) vectors, can we add real-valued noise to the encryption?
- We can take advantage of soft-decision decoding of LDPC codes
- Can soft information be exploited by attackers?

Can state-of-the-art capacity achieving codes, such as spatially coupled LDPC codes [7], be employed successfully? Can they achieve CCA2 security?
- Are such codes (asymptotically) resistant to reaction attacks?
- Can attackers take advantage of encryption memory

RESEARCH NEEDS

- Motivated students
- Cryptography expertise
- Implementation of known attacks to test new designs
- Theoretical analysis and design of QC-MDPC codes and SC-MDPC codes
- HPC and/or GPU programming for compute-intensive simulations
FUNDING SOURCES

- National Science Foundation, “Coding for 5G and Beyond: Limits and Efficient Algorithms.”

- National Aeronautics and Space Administration, “Hybrid UWB/Optical Communications for Distributed Space Systems.”

- National Science Foundation, “The New Mexico SMART Grid Center: Sustainable, Modular, Adaptive, Resilient, and Transactive.” (Networking sub-project collaborator at SNL: Ross Guttromson.)
Research Spotlight Forum
6.4.19 Quantum Information Sciences

The Center for Quantum Information and Control (CQuIC)

PRESENTED BY:
Ivan H. Deutsch, Director of the Center for Quantum Information and Control, Department of Physics and Astronomy, University of New Mexico
Quantum Information Science has a long history at UNM, going back to 1995 when Caves and Deutsch formed the “Information Physics Group” with the Center for Advanced Studies.

* Mike Nielsen: UNM PhD 1998
* Ike Chuang: Los Alamos Postdoc 1997-98
Short Course in Quantum Information

Prof. Ivan H. Deutsch
Dept. of Physics and Astronomy
Center for Advanced Studies
University of New Mexico

Information Physics Group: http://info.phys.unm.edu
ABOUT CQuIC: History

- Quantum Information Science has a long history at UNM, going back to 1995 when Caves and Deutsch formed the “Information Physics Group” with the Center for Advanced Studies.

- In 2009 the Center for Quantum Information and Control (CQuIC) was created, funded by the National Science Foundation.

- In 2016 CQuIC became an NSF-funded Focused Research Hub in Theoretical Physics (FRHTP) – one of two in the nation.
ABOUT CQuIC: Mission and Focus

- An interdisciplinary center for Quantum Information Science bringing together physics, chemistry, and information science for fundamental studies and applications in computation, simulations, and communication, and metrology.

- Research Focus Areas
  - Quantum Information Theory
  - Quantum Optics / AMO Physics
    - Quantum Computation
    - Quantum Simulation
  - Quantum Communication
  - Quantum Metrology

- Key Words
ABOUT CQuIC: Core Faculty

T. Albash  
ECE

S. R. Atlas  
P&A/CCB

F. E. Becerra  
P&A/OSE

C. M. Caves  
P&A

E. J. Crosson  
P&A/CS

A. Miyake  
P&A
ABOUT CQuIC: National Laboratory Adjunct/Research Faculty

A. Baczewski  G. Biedermann  R. Blume-Kohout  Y-Y. Jau
A. Landahl  S. Carr  P. Schwindt
M. Boshier  P. Coles  R. Somma
National Science Foundation
Focused Research Hub in Theoretical Physics

FRHTP Postdocs

Chris Jackson  Raf Alexander  Sayonee Ray  Pablo Poggi
Outreach to scientific community: CQuIC is the administrative home of the Southwest Quantum Information and Technology (SQuInT) Network (27 node institutions) and organizer of the SQuInT Annual Workshop.

Founding organizer: Ivan Deutsch 1997-2016
Chief organizer: Akimasa Miyake, 2016-present
ABOUT CQuIC: SQuInT

21st SQuInT Annual Workshop, Albuquerque NM
ABOUT Akimasa Miyake

• Brief biography:
PhD in Physics, University of Tokyo
Associate Professor of Physics & Astronomy, UNM.

• Research areas:
Theory of quantum computation, simulation, software, algorithms.

Keywords:
List keywords related to your work and research interests:
quantum computation, many-body simulation, software, ion-trap QIP, and NISQ applications.
Briefly describe the current work you do in this area or in areas that might be supplemental to this area.

- **Making a practical 50-qubit quantum computer with ion-trap quantum technology**

  Miyake contributions are (i) co-designing the hardware and software for the best computational performance, and (ii) developing near-term quantum algorithms and applications which function without quantum error correction.

  NSF STAQ Project
Briefly describe the current work you do in this area or in areas that might be supplemental to this area.

• **Making a practical 50-qubit quantum computer with ion-trap quantum technology**
  Miyake contributions are (i) co-designing the hardware and software for the best computational performance, and (ii) developing near-term quantum algorithms and applications which function without quantum error correction.

• **Analyzing physics and complexity of many-body entangled states**
  Tensor network descriptions and other new variational tools like machine learning.
ABOUT F. Elohim Becerra

• Brief biography:

PhD in Physics, University of Maryland
Assistant Professor of Physics & Astronomy, UNM.

• Research areas:

Experimental quantum optics and AMO physics. Quantum communication and networking.

Keywords:

List keywords related to your work and research interests:

Quantum optics, laser cooled atoms, quantum memory, single photon counting, quantum channel capacity,
Multi-state discrimination: Optimized Strategies

Strategy
- Photon number resolving (PNR) detection
- Single-shot measurements

Optimized Displacement


Atom-Photon interfaces: Sources and Memories

*Photons from Four Wave Mixing (FWM)*
ABOUT E. Crosson

• Brief biography:
PhD in Physics, University of Washington
Assistant Professor of Physics & Astronomy and Computer Science, UNM.

• Research areas:
Theory of Quantum Computation, Hamiltonian Complexity, Quantum Error Correction, Quantum Algorithms, Quantum Simulation

Keywords:
List keywords related to your work and research interests:
quantum computation, quantum annealing, complexity, algorithms, quantum machine learning
For over 40 years QMC has been applied to computational studies of spin chains, but the convergence was only understood heuristically.

In 2018, Crosson and Harrow theoretically justified the success of QMC for spin chains without a sign problem by rigorously analyzing the convergence of the path integral QMC Markov chain.

\[
H = \sum_{i=1}^{n} \alpha_{i,i+1} Z_i Z_{i+1} + \sum_{i=1}^{n} b_i Z_i + \sum_{i=1}^{n} \Gamma_{i} X_i + \sum_{i=1}^{n} g_{i,i+1} (X_i X_{i+1} + Y_i Y_{i+1})
\]

CURRENT WORK IN QUANTUM INFORMATION SCIENCES - Crosson

It is an open question whether there exists good quantum stabilizer codes (linear distance, constant rate) with low-weight (local) stabilizer generators. The conjecture that such codes exist is the Quantum LDPC conjecture.

Crosson, with collaborators at Caltech and UC Berkeley, recently gave the first example of almost-good codes with local checks, albeit using approximate codes with noncommuting local constraints.

Besides a new framework for building local checks for any quantum codes with efficient encoding circuits, this work also introduced a new methods for analyzing spectral gaps of high-dimensional quantum spin systems.

Quantum Error Correction

• Brief biography:
PhD in Chemical Physics, Harvard University
Research Professor of Physics & Astronomy and Chemistry & Chemical Biology, UNM.

• Research areas:
Quantum chemistry, materials, density-functional theory, high-performance computing

Keywords:
List keywords related to your work and research interests:
quantum computation for quantum chemistry, high-performance computing, machine learning
Atlas lab (Susan R. Atlas, Physics & Astronomy):

Quantum Chemistry: Design and implementation of principled models for density functional theory (DFT) electronic structure calculations of molecules and materials. The objective is to utilize qubit entanglement to model spatially-complex quantum correlations between electrons and encode the correlations as nonlocal density functionals. Unlike most quantum chemical methods, DFT is formally based on the 3D electron density rather than the many-electron wave function.

Two approaches are being explored:

(1) data analysis of pair interaction patterns in the exchange-correlation energy, using machine learning and data modeling algorithms tailored for quantum computers, and applied to large chemical datasets; and

(2) implementation of nonlocal functionals embodying explicit frequency and wave vector response.
ABOUT T. Albash

• Brief biography:
PhD Physics, University of Southern California
Assistant Professor of Electrical & Computer Engineering, UNM.

• Research areas:
Theory of adiabatic quantum computing, heuristic quantum algorithms, quantum simulation

Keywords:
List keywords related to your work and research interests:
Quantum Algorithms, quantum simulation, optimization, NISQ
T. Albash Research Overview

• Characterizing and benchmarking quantum annealers
  ◦ Scaling requirements for implementation errors (Quantum Sci. Technol. 4 02LT03 (2019))
  ◦ First demonstration of optimal annealing times and true performance assessment for a D-Wave processor (Phys. Rev. X 8, 031016 (2018))
  ◦ IARPA’s QEO Performer Team Task 3 “Verification and Validation” Leader

Role of non-stoquasticity in quantum adiabatic optimization
  ◦ New example of exponential speedup over stoquastic counterpart (Phys. Rev. A 99, 042334 (2019))

Quantum Monte Carlo implementations
  ◦ New quantum Monte Carlo algorithm (Phys. Rev. E 96, 063309 (2017))
ABOUT I. H. Deutsch

• Brief biography:
PhD in Physics, UC Berkeley, Regents’ Professor of Physics & Astronomy, UNM.
Director Center for Quantum Information and Control (CQuIC)

• Research areas:
QI in AMO systems, quantum control and measurement, quantum complexity and simulation.

Keywords:
List keywords related to your work and research interests:
Quantum control, quantum measurement, quantum tomography, quantum optics, quantum simulation, quantum chaos. Rydberg atoms, boson sampling, spin squeezing.
CURRENT WORK IN QUANTUM INFORMATION SCIENCES - Deutsch

Quantum Control of Atomic Spins

Quantum Computational Supremacy in Quantum Simulation

Building Quantum Information Processors

Biedermann
Sandia
CURRENT WORK IN QUANTUM INFORMATION SCIENCES - Deutsch

Seeking answers to the Big Questions

“A major challenge for research using analog quantum simulators is identifying accessible properties of quantum systems which are robust with respect to error, yet are also hard to simulate classically.”

CURRENT WORK IN QUANTUM INFORMATION SCIENCES - Deutsch

Seeking answers to the Big Questions

“A major challenge for research using analog quantum simulators is identifying accessible properties of quantum systems which are robust with respect to error, yet are also hard to simulate classically.”


Entanglement – The Dual-Edged Sword

- Entanglement within system - complex matter.

- Entanglement with environment - decoherence.
CURRENT WORK IN QUANTUM INFORMATION SCIENCES - Deutsch

Seeking answers to the Big Questions

“A major challenge for research using analog quantum simulators is identifying accessible properties of quantum systems which are robust with respect to error, yet are also hard to simulate classically.”


**Big Question:** What is the relationship between robustness and complexity?
- Are “complex systems” hypersensitive to imperfections?
- Are “robust systems” efficiently simulatable?
- What are the implications for analog quantum simulation?
- What are the implications for the natural world?

**Entanglement – The Dual-Edged Sword**

- Entanglement within system - complex matter.
- Entanglement with environment - decoherence.
CURRENT WORK IN QUANTUM INFORMATION SCIENCES - Deutsch

Quantum Complexity

**Kinematic Complexity:**
- Hilbert space dimension grows exponential large with number of subsystems.
- Information stored in *correlations* (entanglement).

**Dynamical Complexity:**
- Information stored locally is “scrambled” nonlocally.
- Quantum chaos and hypersensitivity to perturbations.
- Kolmogorov-Sinai Entropy

**Computational Complexity**
- Polynomial hierarchy
- Quantum computational power
CQuIC’s current total funding is about $5 M

The source are given below: $2.5M
- Internal UNM (College of Arts & Sciences)
- Center-wide Funding
  - NSF FRHP Center Grant
  - NSF NRT (pending)
- Individual investigators - Total $2.5M
  - NSF TAMOP, PI: Deutsch
  - NSF QIS, PI: Miyake
  - NSF CAREER, PI: Becerra
  - NSF STAQ, PI: Miyake
  - NSF QIS, PI: Deutsch
  - Sandia Academic Alliance, PI: Deutsch
  - IARPA QEO, PI; Crosson
  - Google Focus, Co-PIs: Deutsch & Miyake
  - Google Focus, PI: Crosson
RESEARCH NEEDS

Making the Academic Alliance Work

- Not just about individual investigators – about joint programs
- Role of PhD students – research at Sandia National Labs
- Workforce development – creating the pipeline of a “quantum smart” workforce
- A vision for the National Quantum Initiative
Lessons from Quantum Annealing for the NISQ Era

Presented by:
Tameem Albash
Electrical and Computer Engineering, CQuIC, @UNM (Fall 2019)
talbash@unm.edu
SUMMARY OF MYSELF

• Currently at ISI@USC but will be moving to UNM in the fall.

• I started in QIS as part of the USC team when Lockheed-Martin installed the first D-Wave quantum annealing processor at ISI, where I played a role in developing open-quantum-system simulations and benchmarking tools to detect signatures of ‘quantumness’ on these devices. Currently part of the performer team of IARPA’s Quantum Enhanced Optimization (QEO) program.

• While much of my focus to date has been on the adiabatic paradigm of quantum computing, I hope to leverage many of the important lessons we have learned in the adiabatic approach to explore various aspects of the performance of quantum algorithms in the NISQ era.

Keywords:
Adiabatic quantum computing, variational quantum algorithms, quantum simulation
FUNDING SOURCES

• IARPA: Quantum Enhanced Optimization (QEO)
  ➢ “QEO seeks to harness quantum effects required to enhance quantum annealing solutions to hard combinatorial optimization problems. The physics underlying quantum enhancement will be corroborated by design and demonstration of research-scale annealing test beds comprised of novel superconducting qubits, architectures, and operating procedures. All work will serve to demonstrate a plausible path to enhancement and a basis for design of application-scale quantum annealers.”

• Performer team is a multi-university, government, and industry collaboration:
CURRENT WORK IN QUANTUM INFORMATION SCIENCES:
TALES FROM THE TRENCHES OF QUANTUM ANNEALING

• Why did we think quantum annealing was the easiest path for demonstrating the usefulness of specialized quantum computing
• Summary of some of the many problems we encountered along the way
• What excites me and opportunities moving forward
WHY MIGHT QUANTUM ANNEALING BE A PROMISING APPROACH

• An algorithm from the adiabatic paradigm quantum computing (1), whose sole purpose is to solve for the ground state of a ‘classical’ (diagonal in the computational basis) Hamiltonian

\[ H(s) = -(1 - s) \sum_i \sigma_i^x + s H_p, \quad s = t/t_f \in [0,1] \]

• Adiabatic evolution guarantees high success. Only requires slow anneal of all qubits.
• Only requires measurements when the Hamiltonian is classical (at \( s = 1 \)).

• Ground state evolution
  • thermal relaxation can only help.
  • dephasing in instantaneous energy eigenbasis is fine.

• Perturbations to the annealing path are often okay (often referred to as unitary control errors). We will however see problems with this later.

• \( H_p \) is often taken to be an Ising Hamiltonian. Many combinatorial optimization problems can be easily cast as Ising Hamiltonians (2), so there are a lot of applications that can be easily mapped to it.

BE VERY SKEPTICAL OF SMALL PROBLEMS

• Our ability to classically simulate quantum evolution restricts us to small system sizes. Typical small problems (∼20 qubits) tend to be artificially easy.

➢ Studying small system sizes may lead you to believe that the scaling of the algorithm is polynomial (1), when in fact it transitions to an exponential at larger sizes (2).

• At small sizes, running adiabatically may not be optimal. Fast repeated anneals more advantageous.

Algorithmic performance on small problems may not be representative of performance at larger problem sizes!

Most problems are not amenable to any analytical analysis.
How do we determine the algorithm’s performance?
 Seems like we are stuck with building the device in order to find out.

THE PROBLEM OF TEMPERATURE

• Even under most innocuous decoherence model (weak coupling limit master equation), temperature remains a severe impediment to performance.

➢ At too high temperatures, thermal hopping dominates over quantum tunneling as the mechanism of overcoming energy barriers, resulting in measurable differences in performance. To ‘observe’ this (1):

➢ Identify instances for which a semiclassical limit (spin-vector Monte Carlo) encounters discontinuous jumps in the global minimum of the energy landscape. An adiabatic evolution would tunnel through this barrier.

➢ Perform quantum Monte Carlo simulations at high and low temperatures, in order to favor thermal hopping over the energy barrier versus tunneling through the energy barrier.

THE PROBLEM OF TEMPERATURE

- Even under most innocuous decoherence model (weak coupling limit master equation), temperature remains a severe impediment to scalability.

➢ In with a thermal environment for a long time means system approaches the Gibbs state (1) and not the ground state. Probability of finding the ground state now depends on weight of the ground state in the Gibbs state.

\[ H_R = H_P - E_0 \]

Residual energy measures distance (in energy) from the ground state. Residual energy distribution for the Gibbs state becomes more Gaussian like for increasing system size at a fixed temperature.

For Gibbs states with residual energy distributions whose mean grows as \( n \) and whose standard deviation grows as \( \sqrt{n} \), it becomes exponentially unlikely to sample the ground state (2).

---


THE PROBLEM OF IMPLEMENTATION ERRORS

- Implementation of final Hamiltonian is critical. Small deviations in the final Hamiltonian results in a different ground state.
  - Adiabatic evolution, even if ideal, results in the wrong solution!

\[
H_P \rightarrow \sum_i (h_i + \delta h_i)\sigma_i^z + \sum_{\langle i,j \rangle} (J_{ij} + \delta J_{ij})\sigma_i^z\sigma_j^z
\]

Median probability that the ground state remains unchanged when introducing Gaussian noise ($\mu = 0, \sigma^2$) on the Ising parameters as the problem size is scaled.

Probability that ground state remains unchanged scales down exponentially in the system size for a fixed noise level $\sigma$.

(1) TA, V. Martin-Mayor, I. Hen, Quantum Sci. Technol. 4 02LT03 (2019)
THE PROBLEM OF IMPLEMENTATION ERRORS

- Annealing schedules that slow down near the minimum gap require precise control
- Consider the optimal annealing schedule of Roland & Cerf for unstructured search (Grover) (1). The linear annealing schedule is modified such that $s(t/t_f)$ is a non-trivial function
- Optimal schedule is ‘finely’ tuned to the location of the minimum gap. If the minimum gap shifts, then the quadratic speedup is lost.

Optimal annealing schedule becomes exponentially slow (with the system size) near the minimum gap at $s = \frac{1}{2}$

Success of adiabatic evolution decreases exponentially (2) with system size when the minimum gap is shifted away from $s = \frac{1}{2}$ to $s_*$

LESSONS FOR THE NISQ ERA

• It is not surprising that in the absence of error correction, performance does not scale.

• Our devices will always have finite size. Errors need only be as small as necessary for the circuits we want to implement.

• Specialized devices to mitigate errors (co-design): algorithms specialized for a given architecture / architectures tailored for a specific algorithm. Reduces overhead of ‘embedding’ the problem on the device, as well as maximally utilizing ‘native’ hardware capabilities.

• At small sizes, ‘typical’ instances may not be representative of ‘typical’ instances at larger sizes. At small sizes, we should search for the hardest instances to truly understand the limitations of our algorithms and devices.

• Optimism is great, but proper benchmarking against the best classical algorithms is necessary. The goal post is constantly moving, but that’s progress!
WHAT EXCITES ME: NON-STOQUASTICITY

• Standard quantum annealing implements a ‘stoquastic’ Hamiltonian along the entire anneal.
• Definition: all the off-diagonal elements of the Hamiltonian in the computational basis are $\leq 0$. This is basis dependent, so the definition is up to local transformations of the basis.

$$H(s) = -(1 - s) \sum_i \sigma_i^x + \lambda s(1 - s) \sum_{i,j} \sigma_i^x \sigma_j^x + s H_p,$$

$$s = \frac{t}{t_f} \in [0,1]$$

$\lambda \leq 0$, obviously stoquastic

$\lambda > 0$, possibly non-stoquastic

• One of the key differences is that the ground state of stoquastic Hamiltonians have only positive amplitudes, whereas the ground states of non-stoquastic Hamiltonians can have complex amplitudes.

• We know that universal adiabatic quantum computing requires non-stoquastic interactions (1).

• Can using such interactions make (non-standard) quantum annealing more powerful?
  ➢ Typically, these interactions make quantum annealing less efficient (2,3)!
  ➢ Only for very rare situations does non-stoquasticity appear to help (4,5). Of the examples we know, the advantage over its stoquastic counterpart is exponential!

(2) E. Crosson et al., arXiv:1401.7320
WHAT EXCITES ME: NON-STOQUASTICITY

- Exponential advantage appears to be correlated to the fact that the ground state has more flexibility by allowing for arbitrary amplitudes (1).

- Can we better understand when non-stoquastic interactions can help in quantum adiabatic optimization? Our studies so far show that it is definitely not the typical case.

- Non-stoquastic Hamiltonians are generally very interesting. These are associated with the sign-problem in quantum Monte Carlo. Any progress in this direction will likely have far-reaching implications.

- As part of QEO, we hope to build systems that implement such interactions using superconducting Josephson Phase-Slip Qubits (2). So far these qubits are very sensitive to charge noise, and a lot of progress needs to be made before they are ‘device-ready’.

Quantum simulation remains one of the most interesting applications for quantum computing.

Simulation of non-stoquastic Hamiltonians is highly appealing.
- Fermionic systems in condensed matter physics, quantum chemistry, high energy physics, …
- Sign-problem problems: quantum Monte Carlo techniques fail!
- Other algorithms are agnostic to this: Neural/Tensor network approaches. Suggests that not all non-stoquastic systems are hard to simulate. When they do get hard (when long-range entanglement is present) is also when we might expect our quantum device to be challenged.

Suggests there is an open question to be addressed about when we can meaningfully (in the absence of fault tolerant error correction) beat classical simulations of such systems.

Proper benchmarking needs to be done to make meaningful comparisons.
SOME SPECULATION

So far, experience has taught us that whenever things get interesting from a quantum point of view, things also get challenging experimentally (1). Is there something fundamental about robustness/sensitivity and a demonstration of a quantum advantage?

<table>
<thead>
<tr>
<th>Classically Easy</th>
<th>Classically Hard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Experimentally Quantum Robust</td>
<td>Highly likely?</td>
</tr>
<tr>
<td>Experimentally Quantum Sensitive</td>
<td>Useful for verification?</td>
</tr>
</tbody>
</table>

Simulating non-stoquasticity systems seems to be the ideal playground to explore such questions.

RESEARCH NEEDS

• Benchmarking quantum simulation will require a broad range of simulation and algorithmic techniques. We could try to build these in-house, but this is an excellent (and easy) opportunity for collaboration.

• Connecting to applications of interest to the ‘real world’ requires domain expertise. Interdisciplinary should be more than just a buzz word.

• Understanding the quantum information processor is key to understanding and improving its performance (especially for error mitigation/suppression before full quantum error correction). Opportunities for lots of open-quantum system modeling and interactions with experimentalists.

A great example combining all these features:
IBM’s recent-ish VQE paper (Nature 549, 242 (2017))
Used domain expertise to map relevant degrees of freedom of H₂, LiH, BeH₂ to 5 qubits, open quantum system simulations give excellent agreement with device output, showing how decoherence is a significant limiter of performance
GTRI Quantum System Division Overview

PRESENTED BY:

Craig R. Clark, GTRI, CIPHER Lab, Quantum System Division
About GTRI

Georgia Institute of Technology

- Education
- Basic & Applied Research
- Open Environment
  - Unclassified
  - International
- Entrepreneurship & Start-ups

Georgia Tech Research Institute

- Applied Research & Development
- Technology & Systems Prototyping
- Research Space: > 1 million ft²
  - Field Sites: 18
  - Laboratories: 8
- Department of Defense University Affiliated Research Center (UARC)
About QSD

25 Research Scientists

19 PhD’s, mostly in AMO physics (also Optics, Mathematics, Chemistry, and Chemical Engineering)
6 other advanced degree (Mechanical Engineering, Electrical Engineering, Mathematics, other physics)
Extensive AMO lab spaces, HPC capability, GT fabrication facilities

Research programs

Magnetometers (fabrication, physics techniques, and applications)

Laser cooled atoms on chip (on-chip microwave waveguides for matter-wave interferometer)

Permanent magnetic penning trap (atomic clock)

Surface electrode ion traps (experts in ion-transport, programs in quantum information, atomic clocks, chip-design, microfabrication, modeling, and proof-of-concept designs)

Mass Spectrometers and devices for chemical sensing

Research Spotlight Forum
<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Education and Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alexa Harter</td>
<td>CIPHER lab director</td>
<td>B.S., Physics and Mathematics, Brown Ph.D. in Physics,Caltech, 2000</td>
</tr>
<tr>
<td>Curtis Volin</td>
<td>QS Division Chief</td>
<td>B.S., Applied and Engineering Physics, Cornell Ph.D. in Optical Sciences, U. of Arizona, 2000</td>
</tr>
<tr>
<td>Robert Wyllie</td>
<td>QS Associate Division Chief</td>
<td>B.S., Physics, Denison University Ph.D. in Physics, U. of Wisconsin, 2012 Postdoc in Neutral Atom Group, NIST-Gaithersburg</td>
</tr>
<tr>
<td>Kenton Brown</td>
<td>QS Chief Scientist</td>
<td>B.S., Physics, Yale Ph.D. in Physics, U. of Maryland, 2006 Postdoc with David Wineland, NIST-Boulder</td>
</tr>
<tr>
<td>Greg Mohler</td>
<td>QS Chief Engineer</td>
<td>B.S., Physics, Purdue University Ph.D. in Physics, Ohio State, 2001</td>
</tr>
<tr>
<td>J. True Merrill</td>
<td>Theory Branch Head</td>
<td>Ph.D. in Physical Chemistry, Georgia Tech, 2013</td>
</tr>
<tr>
<td>Brian Sawyer</td>
<td>Experiment Branch Head</td>
<td>B.S., Physics, University of Arkansas Ph.D. in Physics, U. of Maryland, 2006 Postdoc with David Wineland, NIST-Boulder</td>
</tr>
<tr>
<td>Adam Meier</td>
<td>Validation and Verification</td>
<td>B.A., Mathematics, B.S., Physics, Rice University Ph.D. in Physics, U. Colorado- Boulder, 2013</td>
</tr>
<tr>
<td>Nicholas Guise</td>
<td>Ion experiment, communications</td>
<td>B.S. Physics, Cal Tech Ph.D. in Physics, Harvard, 2010 Postdoc in the Atomic Spectroscopy Group, NIST-Gaithersburg</td>
</tr>
<tr>
<td>Harley Hayden</td>
<td>Fabrication</td>
<td>Ph.D. in Chemical Engineering, Georgia Tech, 2008 Postdoc at Georgia Tech, NRC</td>
</tr>
<tr>
<td>Creston Herold</td>
<td>Ion and Atom experiment</td>
<td>B.A., Physics and Chemistry, Williams College Ph.D. in U. of Maryland, 2014</td>
</tr>
<tr>
<td>Jonathan Andresen</td>
<td>Quantum Noise</td>
<td>Ph.D. in Physics, Northwestern, 2009 Postdoc, University of Arizona Postdoc, Universite de Nice-Sophia Antipolis</td>
</tr>
<tr>
<td>Clayton Kerce</td>
<td>ML, Classical optimization</td>
<td>B.S., Applied Mathematics, Georgia Tech Ph.D. in Mathematics, Georgia Tech, 2000</td>
</tr>
<tr>
<td>Kelly Stevens</td>
<td>Theory</td>
<td>M.S. in Mathematics, Virginia Tech, 2004</td>
</tr>
<tr>
<td>Christopher Shappert</td>
<td>Mechanical Analysis &amp; Ion Trap Experiment</td>
<td>M.S. in Mechanical Engineering, U. Illinois-UC, 1997</td>
</tr>
<tr>
<td>Wade Rellergert</td>
<td>Mass spectrometry</td>
<td>B.S. Physics, Mathematics, University of Missouri Ph.D., Physics, Yale</td>
</tr>
<tr>
<td>Craig Clark</td>
<td>Ion trap experiment</td>
<td>B.S., Chemistry, Math, Kennesaw State University Ph.D., Chemistry, Georgia Tech, 2011 Post-Doc, Sandia National Laboratories</td>
</tr>
<tr>
<td>Christopher Seck</td>
<td>Ion trap experiment</td>
<td>B.S., Physics, California Polytechnic State University Ph.D., Physics, Northwestern University, 2016</td>
</tr>
<tr>
<td>Karl Burkhardt</td>
<td>Ion trap experiment</td>
<td>B.S., Physics, Georgia Tech M.S., Chemistry, University of Texas</td>
</tr>
<tr>
<td>Brian McMahon</td>
<td>Ion trap experiment</td>
<td>B.S., Physics, Georgia Tech Ph.D. [in process], Georgia Tech</td>
</tr>
<tr>
<td>Yatis Dodia</td>
<td>Electronics and signal processing</td>
<td>B.S., Physics, Georgia Tech B.S., M.S., Electrical Engineering, Georgia Tech</td>
</tr>
<tr>
<td>Abigail Perry</td>
<td>Magnetometer experiment</td>
<td>B.A., Physics, Wellesley College Ph.D., Physics, University of Maryland, 2015 Post-Doc, CU-Boulder/NIST-Boulder</td>
</tr>
<tr>
<td>Holly Tinkey</td>
<td>ion trap experiment</td>
<td>B.S., Physics, Georgia Tech M.S., Physics, University of Maryland, 2014</td>
</tr>
<tr>
<td>Roger Brown</td>
<td>Sensors and ions experiment</td>
<td>B.S., Engineering Physics, Colorado School of Mines Ph.D., Physics, University of Maryland, 2014 Post-Doc, NIST-Boulder</td>
</tr>
<tr>
<td>Robert Clark</td>
<td>Ion traps, communications</td>
<td>B.S., Physics, Chemistry, Ohio Northern Univ. Ph.D., Physics, MIT, 2009 Post-Doc, UT-Austin</td>
</tr>
<tr>
<td>Wesley Robertson</td>
<td>Sensors and ions experiment</td>
<td>B.S., Physics, University of Tennessee Ph.D., Physics, Emory University, 2010 Post-Doc, Max Planck Institute</td>
</tr>
</tbody>
</table>
Quantum Information: Ion Trap design and fabrication

Advanced design and optimization
- Trap design uses in-house codes for optimization, allows the design of novel trap features
- Codes also allow dynamic potentials and efficient ion transport

Splitting and merging of four Ca+ ions

Loading and merging of Ca+ ions

Long chains of Ca+ ions

Yb+ ions in a junction trap
Quantum Information: Ion Trap design and fabrication

Surface electrode trap design

- Designed multiple generations of surface traps, delivered to academic collaborators
- Fabricated at GT and Honeywell
- BGA trap for improved optical access

Doret, C. S. et al., Controlling trapping potentials and stray electric fields in a microfabricated ion trap through design and compensations, *New Journal of Physics* 14, 073012 (2012).

Quantum Information: Ion Trap design and fabrication

Feature integration
- Integrated optics: bulk and diffractive mirrors for fluorescence detection
- Microwave lines for state manipulation

Kielpinski, D. et al., Integrated optics architecture for trapped-ion quantum information processing, Quantum Information Processing 15, 5315 (2016).


Quantum Information: Previous Verification Results

Objectives

- Assess the quality of quantum operations for computing/sensing
- Simulate and verify the effects of noise and control errors on quantum operations
- Understand the impact of noise and control errors on quantum algorithm
quantum spectroscopy and reconstruction of injected (intentionally introduced) magnetic field noise
Quantum Information: Previous Verification Results


---

**Experiment Verification**

**Process tomography of CNOT gate**

---

Experimental test of Robust Phase Estimation (RPE) (calibration) procedure subject to injected errors.
Quantum Information and Algorithms: Demonstrations

Control & Benchmarking

- Ion chain transport for universal control through pairwise addressing
- Wrote compiler to translate quantum circuits to native operations
- 1Q: > 99%
  2Q: > 96%


Impact

- Showed ion transport in surface-electrode traps compatible with high-fidelity algorithm
Impact

- With BV, we obtained 1.10(3) bits of information per query compared to 1 bit classically.
QSD Current Research Interest.

**Quantum Information Science**
- Trap Design and Fabrication
- Quantum Gates
- Trap Operation and Hardware
- Simulation and Evaluation

**Quantum Sensors**
- Penning Ion Trap Clocks
- Atomic Magnetometers
- Magnetic Anomaly Simulation
- Rydberg Atom Antennas
- Trapped Atom Gyroscopes

**Other Research Areas**
- Quantum Secure Communication (QKD)
- Molecular Data Storage (DNA computing)
- Chip Scale Gas Chromatography/Mass Spectrometry
- Random laser Physical Unclonable Functions
Quantum gates: Ion-trap Potential Modulation as an Optical Phase Control

Objective

- Individual qubit addressing crucial in quantum systems like quantum process tomography and quantum communications
- Demonstrate ion-selective high fidelity single qubit gates in ~few ⁴⁰Ca⁺
- Eliminates the need for slow split/merge operations and other downsides of spatially dependent Rabi frequency or differential addressing frequency

Beam Addressing of Ions

Potential Modulation Addressing of Ions

Individual ion addressing in a global beam using trap potential modulation to impart differential phase shifts between ions

Quantum gates: Ion-trap Potential Modulation as an Optical Phase Control

Single ion shuttling

\[ \Delta \phi \sim 2\pi \left( \frac{\Delta d}{1 \, \mu m} \right) \]
**Quantum gates: Ion-trap Potential Modulation as an Optical Phase Control**

**Approach**

- Modify trap potential to apply a differential optical phase to ions
- Benefits: high spatial addressability, fast modification of the spatial phase, uses well established control of trap in segmented surface traps, and no global phase for long multi-well chains.

**future work**

- 1-qubit randomized benchmarking, individually, in the same well
- Quantum process tomography of a 2-qubit Molmer-Sorensen gate
- Implementation of a Toffoli gate and QFT algorithm planned

$$\epsilon < 10^{-2}$$ per gate for each ion
PERMION: Ion clock

- Goal: Reduce Penning trap clock SWaP

- Demonstrate clock operations with $^9\text{Be}^+$ using $^{40}\text{Ca}^+$ as coolant ion

- Low size/weight: NdFeB ring magnets (6500 Gauss at center, 1” magnet spacing)
- Low power: Passive ion confinement (permanent magnets, static voltages)

First Doppler laser cooling in a compact Penning trap (~100 mK)
Optimize magnet gap using Ca spectroscopy as magnetic field sensor

\[
\begin{align*}
\mathbf{B} & \text{ Characterization} \\
(\text{good magnetometer})
\end{align*}
\]
Drift of Ca transition frequency correlates with magnet temperature shift at long times (> 20 min). Magnets were slowly heating due to continuous Ca oven operation.
Goal: Develop fieldable, combined magnetometer and gradiometer, **with high sensitivity in ambient conditions**, useful for better brain imaging

- Vapor cell (Rb vapor, N2 buffer gas, no UHV)
- Lasers (780 nm and 795 nm, “easy”), unique optical setup and pulsed beams
- Magnetometer at zone 1 ($|B_1|$)
- Gradiometer ($\Delta B_{21} = |B_2| - |B_1|$) suppresses common-mode noise

Goal: Develop fieldable, combined magnetometer and gradiometer, with high sensitivity in ambient conditions, useful for better brain imaging

- Vapor cell (Rb vapor, N2 buffer gas, no UHV)
- Lasers (780 nm and 795 nm, “easy”), unique optical setup and pulsed beams
- Magnetometer at zone 1 ($|B_1|$) < 1 pT/√Hz
- Gradiometer ($\Delta B_{21} = |B_2| - |B_1|$) suppresses common-mode noise < 50 fT/cm/√Hz
- fundamental limits (~1 fT/cm/Hz$^{1/2}$ gradient sensitivity)

Atomic Magnetometers/Gradiometer (Northrop Grumman, U-Wisc, Freedom Photonics)
QSD Current Research Interest.

**Quantum Information Science**
- Trap Design and Fabrication
- Quantum Gates
- Trap Operation and Hardware
- Simulation and Evaluation

**Quantum Sensors**
- Penning Ion Trap Clocks
- Atomic Magnetometers
- Magnetic Anomaly Simulation
- Rydberg Atom Antennas
- Trapped Atom Gyroscopes

**Other Research Areas**
- Quantum Secure Communication (QKD)
- Molecular Data Storage (DNA computing)
- Chip Scale Gas Chromatography/Mass Spectrometry
- Random laser Physical Unclonable Functions

Questions?
Moinuddin Qureshi
Architecture and Runtime for Reliable Quantum Computers

PRESENTED BY:

Moinuddin Qureshi,
Professor, ECE, Georgia Institute of Technology
(moin@gatech.edu)
Brief Bio: Moinuddin Qureshi is a Professor of ECE at Georgia Tech. Previously, he was a research staff member (2007-2011) at IBM T.J. Watson Research Center, where he developed the caching algorithms for Power-7 processors. He is a member of the Hall of Fame for ISCA, MICRO, and HPCA. His research has been recognized with the best paper award at MICRO 2018, best paper award at CF 2019, and two awards (and three honorable mentions) at IEEE MICRO Top Picks. His ISCA 2009 paper on Phase Change Memory was awarded the 2019 Persistent Impact Prize in recognition of “exceptional impact on the fields of study related to non-volatile memories”. He was the Program Chair of MICRO 2015 and Selection Committee Co-Chair of Top Picks 2017. He received his Ph.D. (2007) and M.S. (2003) from the University of Texas at Austin.

Research Areas: Computer architecture, specifically:

1. MEMORY SYSTEMS: 3D memories, non-volatile memories, hybrid memories
2. QUANTUM COMPUTING: error mitigation, control processor arch, CRYO
3. HARDWARE SECURITY: cache side channel, secure memory, speculation attacks

Research Group: “Memory Systems Lab” of 5 PhD students

Keywords: Quantum computing, error mitigation, variation-aware qubit mapping, CryoDRAM, Control-processor architecture, cache side channels, integrity trees, mitigating speculation based attacks, stacked DRAM, NVM, Alloy cache, CEASER

Homepage: 
http://moin.ece.gatech.edu/

Group: 
http://memlab.ece.gatech.edu/

Google-Scholar: 
https://tinyurl.com/qureshi-GS
CURRENT WORK IN QUANTUM COMPUTING

OUTLINE

1. Variability-Aware Qubit Mapping for NISQ Computers [ASPLOS 2019]


[Tannu and Qureshi]
Quantum Computers are Here!

Quantum computers can speedup hard problems

 QC with 10+ qubits are here, QC with 100+ qubits expected soon

<table>
<thead>
<tr>
<th>Quantum Machine</th>
<th>Number of Qubits*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>72</td>
</tr>
<tr>
<td>IBM</td>
<td>50</td>
</tr>
<tr>
<td>Intel</td>
<td>49</td>
</tr>
<tr>
<td>Rigetti</td>
<td>19</td>
</tr>
<tr>
<td>IonQ</td>
<td>11</td>
</tr>
</tbody>
</table>

* Under test, fabricated, or announced
Quantum Computing: Background

QC operates on principles of entanglement and superposition

State of qubit is a superposition of state “0” and state “1”

Gate operations modulate state of the qubit
NISQ Programming Model

- Quantum Error Correction is expensive (20x-50x qubits)

- Noisy Intermediate Scale Quantum Computer (NISQ) [Preskill’18]
  - Run program without any error correction

Input Program → Compile → Executable → Execute → Output Log

Repeat for N Trials

Figure of Merit: Probability of Successful Trial (PST)
The Problem of Limited Connectivity

Compiler insert SWAPs $\rightarrow$ SWAPs are extra instructions (can also fail)
NISQ Compiler Policies

Compiler responsible for qubit allocation and movement

Qubit movement policy minimizing SWAPs

Existing compiler policies solely focus on minimizing SWAPs

[1] Zulehner+,(DATE’18)
[2] Siraichi+,(CGO’18)
[3] Li+, (ASPLOS’19)
Not All Qubits Are Created Equal!

- **Variability:** Some qubits and links fail with higher probability than others

- Avoiding certain links can improve reliability significantly

Goal: Exploit variation in error rates to improve reliability (assign more operations on reliable qubits/links)
Characterization Methodology

- Gate operations require analog pulses
- Quantum computers require frequent calibration to get the best pulse
- IBM calibrates machines **multiple times a day and generate the report** contains error rates for each qubit and link
- We analyzed calibration 100+ reports over 52 days for IBMQ-20

<table>
<thead>
<tr>
<th>IBM Q 20 Tokyo</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency (GHz)</td>
<td>4.97</td>
</tr>
<tr>
<td>T1 (μs)</td>
<td>76.91</td>
</tr>
<tr>
<td>T2 (μs)</td>
<td>54.53</td>
</tr>
<tr>
<td>Gate error ($10^{-3}$)</td>
<td>1.73</td>
</tr>
<tr>
<td>Readout error ($10^{-2}$)</td>
<td>9.27</td>
</tr>
<tr>
<td>MultiQubit gate error ($10^{-2}$)</td>
<td>2.88</td>
</tr>
</tbody>
</table>
Two qubit gate error rate is high and show significant variability.
Spatial Variation in Two Qubit (Link) Error Rates

Some links are consistently more error prone than others.

Average link error rate for 76 links in IBM-Q20 machine.

Worst link: 15% CNOT error

Best Link: 2% CNOT error
Variation-Aware Policy

We propose variation-aware policy, to generate initial assignment and operation schedule that maximize the reliability, not just SWAP count.
Qubit Movement

Multiple possible paths to entangle two qubits with identical SWAP cost
Variation-aware Qubit Movement (VQM)

Chose a sequence of swaps that maximizes the reliability
Variation Aware Qubit Allocation (VQA)

Choose qubits that maximizes the reliability

SWAPs = 0  PST = 0.61

SWAPs = 0  PST = 0.77
Evaluations on Real System: IBM-Q5

On IBM-Q5, VQA+VQM improves the reliability up to 1.9x
Evaluations for IBM-Q20 Simulator

VQA+VQM improves PST up to 1.83x over variation-unaware baseline
CURRENT WORK IN QUANTUM COMPUTING

OUTLINE

1. Variability-Aware Qubit Mapping for NISQ Computers [ASPLOS 2019]


[Tannu, Myers, Nair, Carmean, and Qureshi]
http://memlab.ece.gatech.edu/papers/MICRO_2017_1.pdf
Cryogenic Control Processor is essential for scalable Quantum Computer
(Ref: Cryogenic Control Architecture for Large-Scale Quantum Computing by Hornibrook et. al)
Scalable Organization: Thermal Hierarchy

- Host
- Memory (Cryo-CMOS)
- Control Processor
- Quantum Substrate
- Low density metal Interconnects
- High Density Superconducting Control Wires
Quantum bits are fickle

Even at $20mK$, qubits can lose state

Need Error Correction to protect Quantum bits
Quantum Error Correction

- Copying qubits is not allowed
- Measurement destroys the qubit state
- Quantum Error Correction can protect qubits

Continuous Quantum Error is essential to protect the state
Quantum Error Correction

Surface Code
Syndrome Generator
Syndrome Measurement
Data Qubits
Ancilla Qubits
Error

Research Spotlight Forum
Programmable Quantum Error Correction

- Different QECC Designs

- New error correction codes → QECC needs to be programmable

- Software managed QECC → Compiler inserts QECC instructions in regular instruction stream
Baseline Architecture

Uncorrectable Errors!!

Control Processor

Qubits
Problem: Instruction Bandwidth Bottleneck

- Can’t use i-cache -- delay in delivery of QECC instructions results in error

- SW-QECC + no i-cache → instruction bandwidth must scale linearly with number of qubits

Instruction Bandwidth bottleneck → 99.99% of instructions are QECC
QECC Instruction Bandwidth Bloat

- Realistic Quantum workloads require substantially large number of qubits

- Large number of qubits → must support large instruction bandwidth

QECC instruction bloat is dominant in all large scale quantum workloads
**Goal:** To enable programmable Quantum Error Correction without bandwidth bloat

<table>
<thead>
<tr>
<th>Programmability</th>
<th>BW Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>✗</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software-Managed QECC</th>
<th>Hardcoded QECC</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td></td>
<td>✔️</td>
</tr>
</tbody>
</table>
Insight

QECC can be executed independently without any global synchronization

QECC is simple enough to manage in hardware using programmable microcode
Quantum Error Correction Substrate (QuEST)

- μcode engine continuously issues QECC μops
- Master controller issues regular instructions. μcode Engine decodes it to μops

QuEST alleviates instruction bandwidth by issuing QECC ops locally
QuEST -- Organization

300K
Host

77K
Master Controller

4K
MCE MCE MCE MCE
Quantum Substrate

20mK
Quantum Substrate

Run Time Environment

Error Decoder

Quantum Executable

Instruction Pipeline

Error Decoder Pipeline

Microcode Pipeline

Quantum Execution Unit
QuEST reduces global bandwidth demand by seven orders of magnitude.
Key Takeaway for QUEST

<table>
<thead>
<tr>
<th>Programmability</th>
<th>BW Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software-Managed QECC</td>
<td>✅</td>
</tr>
<tr>
<td>Hardcoded QECC</td>
<td>✗</td>
</tr>
<tr>
<td>QuEST (µcode)</td>
<td>✅</td>
</tr>
</tbody>
</table>
CURRENT WORK IN QUANTUM COMPUTING

OUTLINE

1. Variability-Aware Qubit Mapping for NISQ Computers [ASPLOS 2019]


[Tannu, Carmean, and Qureshi]
http://memlab.ece.gatech.edu/papers/MEMSYS_2017_2.pdf
Quantum computers require substantial memory capacity at cryo temperature.

- **Program Memory + Data Memory → Stores**
  - Quantum Executable, Data (~10s GB)

- Memory must be kept at cryo temperature to avoid large thermal gradient

- Josephson Junction technology works at 4K
  - Limited memory density (only few Mb)
Does commodity DRAM work at cryogenic temperatures?

Goal: To characterize a DRAM at cryogenic temperature to understand the functionality and error patterns.
How to Test DRAM at Cryogenic Temperature?

- Conventional memory testing → Memtest86 running on host, dedicated memory testers

- Host machines or memory testers do not work at cryogenic temperatures

Need mechanism to reduce DIMM temperature without affecting tester
Isolated Cooling of DIMM

- Need cryogenic coolant → Liquid Nitrogen (boils at 77K)

- Need isolated cooling of DIMMs → Compact cryogenic heatsink

- DIMM is sandwiched between two heatsinks and can be cooled down to 80K

Compact heatsink with Liquid Nitrogen provides isolated cooling of a DIMM
Challenges: Thermal Shock & Ice Condensation

Limit rate of cooling & use isolation chamber to reduce condensation
Experimental Methodology

- Verify memory functionality by using march-tests
- Fault → single bit fault in a burst
- Minimum Operational Temperature (MOT) → Minimum temperature at which no faults are observed

Number of DIMMS: 55
Number of Chips: 750
Number of Vendors: 5
Minimum Operational Temperature for DIMMs

18% DIMMs are functional below 90K
92% of chips worked at 90K — Pick cryogenic tolerant chips
Fault Granularity

- Single bit errors → Uncorrelated faults
- Linear codes (SECDED, BCH) are still effective

![Single bit fault](99.985%)

![Double bit fault](0.015%)

Uncorrelated faults → Conventional ECC can be effective for Cryo DRAM
Cold DRAM – Take Away

❖ Quantum computers need dense memory at low temperature

❖ Does DRAM Work at cryogenic temperature?

❖ Experiments show → most commodity DRAM chips work at 90K

❖ Error patterns are amenable to existing fault tolerance techniques
FUNDING SOURCES

List funding sources of current projects, if applicable - especially joint work with Sandia, other NM Universities, or other Sandia Academic Alliance Universities (UT Austin, Georgia Tech, UIUC, or Purdue).

➢ NSF and SRC (Hybrid memory research)
➢ Intel (3D memory research)
➢ Microsoft (Gift for research in quantum computing)
RESEARCH NEEDS

Describe any gaps or new directions that would benefit from collaboration.

➢ Access to larger-scale quantum machines and test-bed to test error mitigation algorithms
➢ Access to characterization data for quantum machines to enable new error mitigation algorithms
➢ Access to emerging NISQ algorithms and applications
➢ Funding opportunities (for collaboration and joint works)
Research Spotlight Forum

6.4.19 Quantum Information Sciences

Purdue Quantum Science and Engineering Institute (PQSEI); Quantum Matter/Materials and Devices for Quantum Information Sciences

PRESENTED BY:

Yong P. Chen, Director of PQSEI; yongchen@purdue.edu
ABOUT Myself

- Brief biography: MS in mathematics from MIT (1999), PhD in electrical engineering from Princeton University (2005), and did a postdoc in atomic physics at Rice University. Joined Purdue faculty in 2007, currently Professor of Physics & Astronomy and Electrical & Computer Engineering as well as the Associate Director of Research for Birck Nanotechnology Center, and Inaugural Director of Purdue Quantum Science and Engineering Institute (PQSEI). Assoc. Editor for AIP-AVS Quantum Science and Foreign PI in WPI-AMIR (International Material Research Center) in Tohoku Univ., Japan. Received NSF Career Award, Young Investigator Awards from DOD and ACS, IBM Faculty Award, a Horiba Award in Japan, Villum Investigator Award in Denmark, and an elected APS Fellow (2016).

- Research areas: Experimental condensed matter physics & nanoscience (graphene/2D materials, topological insulators, 2D electrons/quantum Hall physics) and atomic/molecular/optical (AMO)/quantum physics/quantum photonics (cold atom Bose-Einstein condensation, cold molecules)

- Research group (Quantum Matter and Devices Lab: www.physics.purdue.edu/quantum) interests: “Making, Manipulating and Measuring Quantum Matter and Devices” (with potential applications such as energy, sensing and quantum technologies.), typically ~10 people @ Purdue (currently 5 PhD students (both PHYS and ECE), 2 postdocs, 4 undergrad/summer students)


Keywords:

Graphene, 2D materials, topological insulators, spintronics, Josephson junctions, topological superconductors, quantum Hall, plasmonics, photodetectors, radiation detectors, thermal transport, thermoelectrics; Bose-Einstein condensates, cold molecules, photoassociation; topological phases, synthetic gauge fields and spin-orbit coupling; quantum computing; quantum simulation; quantum materials; quantum devices; quantum photonics. see publication profile:

CURRENT WORK IN QUANTUM INFORMATION SCIENCES

Quantum Matter and Devices (QMD) Laboratory – www.physics.purdue.edu/quantum

Graphene/2D materials

Topological insulators/materials

Quantum Optics/AMO physics

Insulator(h-BN); Semiconductor (TMDs – MoS₂, WS₂…); [superconducts/magnets], twisted bilayers/hybrids/vdW heterostructures...

Topological superconductors/semimetals

atomic BEC/superfluids; synthetic gauge fields/ SOC/topological phase

quantum photonics/emitters
A Center for Disruptive Quantum Technologies

(Ultrafast) Quantum Photonics and Quantum Sensing

Quantum photonics:
Pulse-shaping of photons (time/frequency domain)
On-chip generation of Single/entangled photons;
Photonic “qudits” (high-dim) for quantum computing;
Quantum communications/imaging/“quantum radar”

Quantum emitters (single photon sources)
Use plasmonics enhancement and speedup to beat decoherence

Ultrasensitive detectors for:
- Force
- Torque
- Photon
- Radiation
- Magnetic Field
- Nuclear Spins (nanoscale NMR)

Quantum Control and Quantum Energy

Quantum Computing and Quantum Informatics

Quantum materials/devices platforms:
Josephson junctions; quantum dots;
Topological materials/states & topological quantum computation

Quantum & quantum-inspired algorithms for computing speedup,
optimization, data-analytics and machine learning (for wide range of scientific & business applications)

To learn more: [https://engineering.purdue.edu/PQC](https://engineering.purdue.edu/PQC) Email: [PQC@purdue.edu](mailto:PQC@purdue.edu) (yongchen@purdue.edu);
Ultrabright plasmon-assisted single-photon source


Nano-scale magnetometer and NMR sensors

[Shalaev & Boltasseva] All-optical (based on NVs.) & other color-centers [also work by Li]

Photonic quantum communication, computing, memory


Torque and force sensing


Graphene-based photo/radiation-detectors


More information: Yong P. Chen (Director, PQSEI; yongchen@purdue.edu)
Objective:
- Integration of atoms and ions with silicon photonics for realization of strong light-matter interactions on chip

Approach:
- We are investigating cooperative coupling of rare earth ions with photons enhanced by the plasmonic and dielectric mode confinement to realize strong linear and nonlinear light-atom interactions on a hybrid scalable platform.
- We take the loss in the plasmonic structures to our advantage while relying on the strong light confinement to controllably engineer the quantum interactions.
- We work to achieve
  1. Superradiance of ions in Si photonic structures for photon generation
  2. Integration of rare earth crystals with Si photonics for quantum light storage near the telecom wavelength
  3. Implementation of a hybrid dielectric-plasmonic platform for optical storage and processing

Applications:
- Quantum sources and memories for quantum communication
- Photonic logic operation for quantum computation

Fig. High-level schematics of the integrated quantum photonic system

Sandia Collaborator: Edward Bielejec
Quantum Control and Quantum Chemistry

"Quantum chemistry interferometry" using reactants (atoms) in (spin) quantum superposition states

Scattering/Reaction path1
Scattering/Reaction path2

(a) Use spin-sensitive PA that only associate

(b) $\frac{q}{k_{\text{R}}}$

(c) Energy

(d) $\frac{E_{\text{r}}}{E_{\text{r}}}$

(a) Experiment
Theory: No Interference
Destructive Interference

Destructive interference shuts-off the reaction!


Interesting to explore quantum chemistry/catalysis?

Coherent exciton transport in molecules (important for photosynthesis, solar cells...)

Tim Zwier

Libai Huang
Hybrid ("Spintronic") Quantum Materials Platform for Quantum Information [Spintronics-Superconductivity-Quantum Photonics]

- Topological Insulators (Topological Materials)
- Superconductors
- Magnets (FerroMagnet; AntiFerroMagnets; Spin-liquids..)
- Qubits/Qsensors (single spins; Josephson Junctions; NV/color center quantum optical emitters)

(most of these can be realized in 2D/vdW material platforms)
Topological Superconductivity & “Majorana fermions”

Majorana (fermion)

- Neutrino?
- Supersymmetric partner e.g. of photon: photino

... WIMPs (dark matter) ?...

PRL 100, 096407 (2008)
Superconducting Proximity Effect and Majorana Fermions at the Surface of a Topological Insulator

Liang Fu and C. L. Kane
Department of Physics and Astronomy, University of Pennsylvania, Philadelphia, Pennsylvania 19104, USA

$2 \uparrow_{-k}\downarrow_k = (\uparrow_{-k}\downarrow_k + \downarrow_{-k}\uparrow_k) + (\uparrow_{-k}\downarrow_k - \downarrow_{-k}\uparrow_k)$

→ p-wave ($p_x \pm ip_y$) superconductor
→ Majorana “fermion” (anyon)

Spin-helical (“spinless”) fermion + s-wave SC

Other “Majorana” systems:
- Fractional quantum Hall [5/2?]
- $p$-wave superconductor [$Sr_2RuO_4$?...]
- topological superconductor [$Cu_xBi_2Se_3$?]
- s-wave SC/semiconductor (w/t spin-orbit) [InSb,...]
- cold atoms & molecules ......
SC/TI/SC Josephson Junctions & SQUIDs — probe topological superconductors/majoranas

Phase-sensitive measurements: can apply to other “unconventional” or “topological” superconductors

Gate-tunable supercurrent

$I = I(\Delta \phi) = I_c \sin(\Delta \phi)$

(simplest /conventional)

Multiple Andreev Reflection (demo good SC contact quality)

Josephson junctions

M. Kayyalha et al. PRL 122, 047003 (2019)

Anomalous T-dependence of $I_c$

collaborators: L. Rokhinson (Purdue) et al.

Luis A. Jauregui & M. Kayyalha et al. Appl. Phys. Lett. 112, 093105 (2018);
Measurement of Current-Phase Relation (CPR) of S/TI/S

Topological: quasiparticle poisoning → 2π-periodic, yet highly-skewed

Technique: “asymmetric SQUID” [e.g. Rocca et al. PRL’07]

$I_S = I_{C2} \sin(\varphi_2) + I_1 \left( \frac{2\pi \varphi}{\Phi_0} + \varphi \right)$

$\Rightarrow I_{CS}(\Phi) = I_{C2} + I_1 \left( \frac{2\pi \Phi}{\Phi_0} + \frac{\pi}{2} \right)$

( $I_{C2} \gg I_{C1}$ )

Caution: highly-ballistic junction can also gives skewed CPR

Highly-skewed (non-sinusoidal) CPR!

• Low/zero energy ABS ($\varphi = \pi$)?
• Topological SC?

Technique: "asymmetric SQUID" [e.g. Rocca et al. PRL’07]

M. Kayyalha et al. submitted’2018; arXiv:1812.00499

Andreev bound state (ABS) spectrum

Topological: $I(\phi) \sim \sin(\phi)$

Trivial: $I(\phi) \sim \sin(\phi)$ [with scattering]

$T_{sample} = 30 \text{ mK}$
Current major platforms (physical systems) for Majorana & Topological QC

Fractions quantum Hall (FQH) States
[e.g. v=5/2 & related FQH states?]

Spin-orbit-coupled semiconductor Nanowires [e.g. InSb, InAs] + Superconductor (SC)

(pursued at Microsoft Station Q, etc.)

Topological insulator (TI) + Superconductor (SC)

Advantages:
• 2D/surface based devices
[SC islands on surfaces of TI]: easy fabrication & scale-up
• Conceptually simplest, single-particle spin-helical band/transport well established
• No B field or only moderate B fields involved

Challenge: “less friendly” materials (?)

Challenges:
• Complex physics – strongly interacting & correlated many-body states
• Need ultraclean (high mobility) samples
• Ultralow temperature (mK) & high B field

Advantage: well-developed semiconductor (e.g., MBE) based materials/devices/technology ...

Potential Sandia Collaborators: R. Lewis, W. Pan, J. Reno, M. Lilly...
A new frontier & practical application: “quantum speedup” of optimization problems

<using existing “small” quantum computer (“NISQ”) or NISQ+classical computer to solve problems intractable today>

Connection with Krannert school & data-science initiative..

- Logistics Management
- Supplies Chain Management
- Network management
- Fault Diagnostics
- Software/electronics validation/verification
- Artificial Intelligence/Machine Learning
- Blockchain?
- “post-quantum encryption”
- ....


<R.Srivastava et al. NQIT user team report>
(PQSEI) [previously Purdue Quantum Center]

Quantum Materials
- Semiconductors, Superconductors...

Quantum Devices
- Quantum Dots
- Josephson Junctions/SQUIDs

Quantum Photonics
- Quantum emitters (NV, h-BN...)
- Single photons & entangled photons

AMO Physics

Quantum Chemistry

Quantum Control & Measurement

Quantum Simulation

Quantum Info/Computing/Data/Machine Learning

To learn more: PQC@purdue.edu (yongchen@purdue.edu); https://engineering.purdue.edu/PQC
Some “big” questions & interdisciplinary research themes

- **Can topology help store/process/protect** (quantum) info?

- **Can we speedup** (light-matter interaction &) quantum operation to beat decoherence?

- **Using quantum beam/bits** to measure quantum materials

- **“Using chemistry to study physics”**
  (Novel quantum chemistry/catalysis of quantum systems/materials)

- **“Quantum informatics and data analytics”** (speed up science & business?)
  (including “quantum-inspired” algorithms e.g. probabilistic computing/optimization)

To learn more: [https://engineering.purdue.edu/PQC](https://engineering.purdue.edu/PQC) Email: PQC@purdue.edu (yongchen@purdue.edu)
CURRENT WORK IN QUANTUM INFORMATION SCIENCES

http://www.physics.purdue.edu/quantum

Postdoc Openings (yongchen@purdue.edu)

Quantum Synthesis
(➔ novel Quantum matter) + Quantum Measurement & Devices
(➔ manipulation ➔ new quantum technologies)

Graphene & 2D materials

Topological Insulators

Atomic Bose-Einstein Condensate

LiRb Molecules

Research Spotlight Forum
FUNDING SOURCES (current)

1. NIST, Quantum Electronic Metrology In Graphene Nanostructures (2013-2019)
2. NSF EFRI Newlaw: Topological Thermal Transport (2016-2020)
4. NSF (ECCS): Collaborative Research: Strain Based Devices For Switches And Memory Applications (2017-2020)
5. NSF (DMR): Eager: Enabling Quantum Leap: Electrically Tunable, Long-Distance Coherent Coupling Between Room Temperature Qubits Mediated By Magnons In Low-Dimensional Magnets (2018-2020)
   [this project studies NV centers mediated by magnons on magnets]
8. WPI-AIMR/JSPS(Tohoku Univ.): International Joint Research – Quantum Materials and Spintronics (2019-2020)
Making Quantum Materials

Interests: Topological/2D Materials for QIS Applications


2D materials (graphene, TI, h-BN, TMDCs, magnets, superconductors..) & stacked/twisted heterostructures

by CVD & exfoliation/transfer

Nature Nano 11, 345 (2016)

~2D flakes & 1D nanoribbons (CVD & exfoliation)


PRB 98, 035425 (2018)
**Transport/devices**  
[T~10mK to >300K; B to 10-18T @PU, 35-45T in magLab; with back/top/side/ion gate]

1) Charge transport (magneto/QHE)  
2) Coulomb drag  
3) Thermoelectric/thermal

**Optical/Optoelectronics**

1) Raman/PL spectroscopy & mapping (4K-800K, with electrical gating/transport)  
2) Photoconductivity

**OptiMag Cryostat**  
[T~4K, B~5T]

3) Kerr/Faraday Rotation (micro MOKE)
Already at least 4X lower noise than traditional Junctions! (prelim.data, with R.McDermott)

- **TI-based “majorana”/topological qubits** (demo “Fu-Kane proposal” etc.)
  - Better qubits & SQUIDs

TI + (2D) superconductors
Majorana/non-Abelian anyons
→ topological quantum computing

Build material/device platform for Fusing & Braining Majorana
(Josephson junction arrays on TI)

- **2D materials to reduce decoherence/noise in qubits/q-sensors**
e.g. h-BN as dielectric tunnel barrier in Josephson Junctions
  → better qubits & SQUIDs

  h-BN dielectric promises better Josephson junctions (?!):
  - 2D atomic crystal – near perfect lattice and crystallinity
  - Ultralow defects -- (shown to be “best” dielectric)
  - Clean interface with other 2D material superconductors
    → Better qubit (lower decoherence) & sensor (lower noise)

**Other possibilities:** Graphene-passivated superconductor
or 2D superconductor (eg. FeSe) might provide cleaner
Superconductors in Josephson junctions?
Graphene(passivated)-electrodes for low-noise ion trap electrodes?
Potential Project: 2D material (h-BN) based Josephson Junctions: h-BN as dielectric tunnel barrier – better qubits & SQUIDs

Josephson junctions: basis of SQUID and SC-qubits (another leading candidate for quantum computing) -- yet also hard to scale up due to decoherence

Potentially h-BN based Josephson Junctions!

J. Tian et al.

h-BN dielectric promises better Josephson junctions (!):
- 2D atomic crystal – near perfect lattice and crystallinity
- Ultralow defects -- (shown to be “best” dielectric)
- Clean interface with other 2D material superconductors → Better qubit (lower decoherence) & sensor (lower noise)

Graphene-passivated superconductor or 2D superconductor (eg. FeSe) can provide cleaner superconductor too.

Research Spotlight F...
Potential Project 2: Graphene-based electrodes for ion traps

Trapped ions: one of the two leading candidates for quantum computing

Still limited to small number (~10) qubits due to decoherence

Decoherence mainly due to noise (current/field fluctuation) in electrodes (Au) [grains; defects; adsorbates etc.]

Graphene has shown promise to be a new low-noise, ‘clean’ surface conductor free from such issues (single crystalline, inert surface etc.)

CVD single crystal graphene (Chen)

Potential Sandia Collaborators: D.Stick,
Enhanced Graphene Photodetector with Fractal Metasurface

Jieran Fang, Di Wang, Clayton T. DeVault, Ting-Fung Chung, Yong P. Chen, Alexandra Boltaessa, Vladimir M. Shalaev, and Alexander V. Kildishev

School of Electrical and Computer Engineering, Department of Physics and Astronomy, and Birck Nanotechnology Center and Purdue Quantum Center, Purdue University, West Lafayette, Indiana 47907, United States

DTU Fotonik, Department of Photonics Engineering, Technical University of Denmark, Lyngby, DK-2800, Denmark

(a) Optical chopper
(b) Sample 1
(c) Photovoltage (μV)
(d) Photovoltage (μV)

(a) Enhancement
(b) Absorption (%)
(c) Normalized Photovoltage (a.u.)
(d) Photovoltage (μV)

Power = 1 mW
λ = 514 nm

Sample 2

(a) Graphene
(b) Edge

Enhancement
Absorption (%)

Wavelength (nm)
Graphene on SiC as photo-actuated FET ("phototransistor") → **large-area, nonlocal** photodetection/imaging (by few pixels)

Position sensitivity of graphene field effect transistors to X-rays

Edward Cazalas,1,a,b) Bidrit K. Sarker,2,3,b) Michael E. Moore,1 Isaac Childres,2,3
Yong P. Chen,2,3,4 and Igor Jovanovic1
1Department of Mechanical and Nuclear Engineering, The Pennsylvania State University, University Park, Pennsylvania 16802, USA
2Department of Physics and Astronomy, Purdue University, West Lafayette, Indiana 47907, USA
3Burck Nanotechnology Center, Purdue University, West Lafayette, Indiana 47907, USA
4School of Electrical and Computer Engineering, Purdue University, West Lafayette, Indiana 47907, USA
(Received 9 January 2015; accepted 15 May 2015; published online 3 June 2015)
Radiation Response and Radiation hardness of graphene transistors

- High energy electrons ionize e-h pairs in Si wafer
- Less mobile holes trapped at oxide-Si interface, inducing electrons in the channel (graphene)
- Analogous to the well-known negative-shift of threshold voltage in MOSFET subject to high energy ionizing irradiation

Suspended graphene (no substrate): much smaller shift! -- good for rad-hard electronics?! 

I. Childress et al. SPIE proceeding (2011)

Orders of magnitude higher Responsivity than traditional X-ray sensor
(also works for gamma, UV…)

Describe any gaps or new directions that would benefit from collaboration.

- Access to QIS hardware platforms/"testbeds" techniques: trapped ions, Josephson junction QC, single atoms etc.
- Measurement/metrology/testing tools: scanning probe, elemental analysis,
- Processing tools: ion implantation, radiation/beam sources …
- Computational: first principle (DFT+) materials simulation (bands, defects, …)